



United States Department of the Interior

NATIONAL PARK SERVICE

1849 C Street, N.W.
Washington, D.C. 20240

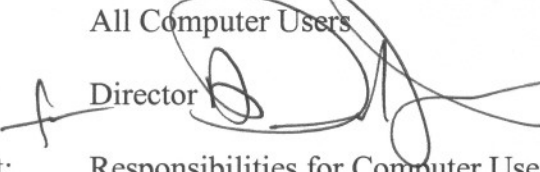
IN REPLY REFER TO:

S72(2550)

NOV - 6 2003

Memorandum

To: All Computer Users

From:  Director

Subject: Responsibilities for Computer Use

Please read the document entitled *Responsibilities for Computer Use* carefully. This document serves several purposes.

It communicates to you a summary of many policies in one place. It is a quick reference for new employees as well for as long-time employees on what is expected and what is prohibited in regards to Information Technology (IT) Security and the use of National Park Service (NPS) computer systems.

The signed acknowledgement form is a document where your supervisor (or, in the case of a contractor, your manager) can validate your need for a user ID.

Lastly, the signed acknowledgement form is the confirmation that a system administrator needs to know that approval has been granted to you for a user ID.

I thank you for the special attention that you pay to this document and for your concerted effort to keep NPS data and systems secure.

Attachment



Responsibilities for Computer Use

Version 2003- 3

This document contains the rules of behavior for the use of NPS Information Technology (IT) Resources.

[blank page]



NPS Computer User's Acknowledgement of Responsibilities

I have read the document entitled "*Responsibilities for Computer Use Version 2003-3.*" I understand that I am responsible for complying with the rules of behavior set forth in the document. I also understand that I am responsible for protecting my NPS account information and agree to report any computer security incidents to the appropriate information security representative.

Print user's name

Signature

Date

Region or Directorate, Park/Center/Office

I certify that the person who signed above is authorized to obtain a user ID for the use of NPS computer equipment, networks, and electronic mail.

Print supervisor's or authorizer's name

Signature

Date

This completed form authorizes a systems administrator to grant you a user ID to an NPS computer network and an e-mail account. The user's supervisor or manager must retain this form.

Unauthorized use of U S Government computer systems is punishable under Title 18, United States Code, Section 1030

[blank page]

Responsibilities for Computer Use

Version 2003- 3

Table of Contents

	NPS Computer User's Acknowledgement of Responsibilities	iii
1.	Introduction	1
1.1	What is the Purpose of This Document?	1
1.2	Who is Covered by the Rules of Behavior?	1
1.3	What are the Penalties for Non- Compliance?	1
2.	Rules of Behavior – General Requirements	2
2.1	Official Business	2
2.2	Access	3
2.3	Accountability	3
2.4	Confidentiality	4
2.5	Integrity	4
2.6	Availability	4
2.7	Passwords and User IDs.....	5
2.8	Hardware	6
2.9	Software	6
2.10	Awareness	7
2.11	Incident Reporting.....	7
3.	Rules of Behavior - Special Circumstances	8
3.1	Privileged Users.....	8
3.2	Work- at- Home and other Remote Users.....	9
3.3	Users who maintain Public Access Sites	9
3.4	Contractors and Non- NPS Employee ('Guest User')	10
4.	User Notes	12

[blank page]

1. Introduction

1.1 What is the Purpose of This Document?

National Park Service information technology resources are the property of the federal government and must be protected. This document explains the requirements as specified by OMB Circular A-130 and other policies and is meant to provide an understanding to users of what is expected from them. Users' access to computing resources indicates a level of trust bestowed upon them by their management and ultimately by NPS. Users are responsible for their actions and must be aware of and acknowledge their responsibilities.

1.2 Who is Covered by the Rules of Behavior?

The NPS rules of behavior apply to all employees who use unclassified systems. In addition, these rules apply to all personnel (e.g., seasonal employees, contractors, and partners) using NPS information technology (IT) resources. All individuals who require a user ID on an NPS system must be aware of their responsibilities and comply with the rules of behavior.

Additional rules of behavior for contractors and other non-NPS employees, and other special considerations are provided in section 3. The rules of behavior do not apply to Union officials conducting Union business.

IT resources refers to electronically-stored information, computer equipment, software, operating systems, storage media, and network accounts providing electronic mail and web browsing.

1.3 What are the Penalties for Non-Compliance?

These rules of behavior are founded on the principles described in the NPS published security policy and other regulatory documents such as the Code of Ethics for Government Employees, Office of Personnel Management regulations, Office of Management and Budget regulations and Standard of Conduct for Federal Employees. Therefore, these rules carry the same responsibility for compliance as the official documents cited above. NPS will apply these penalties in a uniform and consistent fashion regardless of race, sex, color, national origin, disability, religion, marital status, grade level, or bargaining unit status of the personnel involved. Supervisors must exercise sound and reasonable judgment in enforcing these rules of behavior. Penalties must be assessed in a timely manner. NPS will enforce the use of penalties against any user who willfully violates any NPS or federal system security (and related), including:

- Official, written reprimands
- Suspension of system privileges
- Temporary suspension from duty
- Removal from current position
- Termination of employment, and possibly
- Criminal prosecution.

2. Rules of Behavior – General Requirements

The rules of behavior are rules that establish the expected and acceptable behaviors required. Because written guidance cannot cover every contingency, you are also asked to use your best judgment and highest ethical standards to guide your choices and actions. The rules presented in this document highlight requirements from several laws, policies and best practices. More complete information can be researched, if required, by contacting one's supervisor, ethics officer, procurement official or IT security manager.

2.1 Official Business

Employees may use government computers and the Internet for personal use on their own personal time (before and after work, during lunch and during other breaks) provided that there is no additional cost to the government.

Employees may make purchases over the Internet, provided they have the purchased item sent to a non- government address.

The following non- official activities are absolutely prohibited on any government owned or leased computer equipment at any time:

- Gambling
- Intentionally visiting and downloading material from pornographic web sites
- Lobby Congress or any government agency
- Campaigning – political activity
- Online stock trading activities
- Online real estate activities
- Activities that are connected with any type of outside employment
- Endorsement of any products, services or organizations
- Any type of continuous audio or video streaming from commercial, private, news or financial organizations.

Employees have no restrictions on incoming email; however, automatic filters will be in place to help prevent offensive messages from passing through our email gateways.

Employees may send out personal email provided that:

- Any message is not sent to more than five addresses – no mass mailing
- No personal broadcast transmissions.

Users understand that any e- mail on a government e- mail system is the property of the government and may become an official record.

Users consent to monitoring and security testing to ensure proper security procedures and appropriate usage are being observed for NPS IT resources. Monitoring of e- mail and other IT resources by management will only be done in accordance with established NPS policy and guidelines.

The use of these IT resources constitutes possible monitoring and security testing.

Users will not use NPS IT resources for fraudulent or harassing messages, or for unwelcome sexual remarks or materials. Additionally, users shall not send, retain nor proliferate any such material on any Government systems.

2.2 Access

Users shall access and use only information for which they have official authorization.

Follow established procedures for accessing information, including use of user identification, user authentication, passwords, and other physical and logical safeguards.

Follow established channels for requesting and disseminating information.

Access only those files, directories, and applications for which access authorization by the system administrator has been granted. Use government equipment only for approved purposes.

Do not give information to other employees or outside individuals who do not have access authority to it.

Do not store sensitive or confidential information on a system unless access control safeguards (e.g. passwords, locked rooms, protected LAN storage areas) are used.

Do not use your trusted position and access rights to exploit system controls or access data for any reason other than in the performance of official duties.

2.3 Accountability

Users are accountable for actions related to information resources entrusted to them.

Behave in an ethically, technically proficient and trustworthy manner when using systems.

Be alert to threats and vulnerabilities such as malicious programs and viruses.

Prevent others from using your accounts by using procedures such as the following:

- Logout or lock the screen when leaving the vicinity of your terminal or PC
- Set a password on automatic screen savers.

Help remedy security breaches, regardless of who is at fault.

Immediately notify the system administrator whenever there is a change in your role, assignment, or employment status and/or when access to the system is no longer required.

Participate in IT security training and awareness programs.

Don't install or use unauthorized software on NPS equipment.

Comply with all software licensing agreements; don't violate Federal copyright laws.

Practice good citizenship when accessing external systems by complying with that system's rules of behavior.

Read and understand banner pages and end user licensing agreements.

Know that there may be monitoring and that there is no expectation of privacy on NPS IT resources.

2.4 Confidentiality

Access to confidentially sensitive information must be restricted to authorized individuals who need it to conduct their jobs. This entails refraining from intentional disclosure and using measures to guard against accidental disclosure.

Protect confidentially sensitive information. Never access or disclose personal information or other sensitive data unless it is necessary to perform official duties.

Do NOT send highly sensitive information via e- mail or fax, unless encrypted.

Ensure that sensitive information sent to a fax or printer is handled in a secure manner, e.g., cover sheet to contain statement that information being faxed is confidential.

Don't store or transmit confidential information on public- access systems, such as email or the Internet.

Lock up media, such as paper copies, tapes, and disks, containing confidentially sensitive data. Dispose of media according to approved procedures.

Never access someone else's account or files without a supervisor's formal authorization.

2.5 Integrity

Users must protect the integrity and quality of information.

Review quality of information as it is collected, generated, and used to make sure it is accurate, complete, and up to date.

Take appropriate training before using a system to learn how to correctly enter and change data.

Protect information against viruses and similar malicious code by:

- Using virus detection and correction software
- Avoiding unofficial software, such as shareware and public domain software, and
- Discontinuing use of a system at the first sign of virus infection.

Never enter unauthorized, inaccurate, or false information into a system.

2.6 Availability

Computer systems and media must be protected from environmental factors, such as fire, water, heat, and food spills. They must also be protected from theft, unauthorized alteration, and careless handling.

Use physical and logical protective measures to prevent loss of availability of information and systems, such as:

- Ensure that there are backups of information for which you are responsible
- Protect systems and media where information is stored
- Store media in protective jackets

- Keep media away from devices that produce magnetic fields (such as phones, radios and magnets).

Follow contingency plans when necessary.

For important information, ensure that more than one individual knows where to find it and has access rights.

2.7 Passwords and User IDs

Users are responsible and accountable for any actions taken under their user ID.

Protect passwords from access by other individuals.

Never give a password to another person, including your supervisor or a computer support person.

Do not ask anyone else for his or her password.

Construct effective passwords by following NPS rules for complex passwords.

What not to use:

- Don't use your login name, e.g., smithj, in any form (as- is, reversed, capitalized, etc.)
- Don't use your first or last name in any form
- Don't use other information easily obtained about you. This includes license plate numbers, telephone numbers, name of favorite sports team, the brand of your automobile, your spouse's or child's name, etc
- Don't use a word contained in English or foreign language dictionaries, spelling lists, or other lists of words
- Don't use a password shorter than eight characters.

What to use:

- Do use a password with mixed- case letters and with non- alphabetic characters, e.g., digits or punctuation or combine with alphabetic characters, e.g., \$robkoT2!
- Do use a password that you can type quickly, without having to look at the keyboard. This makes it harder for someone to steal your password by watching over your shoulder.

Change passwords at least every 90 days or immediately when they may have been disclosed.

Do not store your password near or on a computer. (If you must write it down, make sure it is kept on your person or in a sealed envelope in a locked cabinet or safe).

Never attempt to bypass or automate login procedures that require user ID and password entry, define them by function keys, or program them into applications.

Be alert to unauthorized attempts to use your user IDs and passwords; immediately report unauthorized access attempts to a security official.

Immediately notify the system administrator whenever there is a change in your role, assignment, or employment status and/or when access to the system is no longer required.

For password requests made on <http://my.nps.gov>

- Only the user should request web passwords

- Unique passwords should be used
- Passwords should be of appropriate strength
- It is inappropriate for one person to enter passwords for other people or for multiple users to have a common password.

2.8 Hardware

Users must protect computer equipment from damage, abuse, theft and unauthorized use.

Protect computer equipment from hazards, such as:

- Extreme temperatures
- Electrical storms
- Water and fire
- Static electricity
- Spills from food and drink
- Dropped objects
- Dust and dirt, and
- Combustible materials.

Keep an inventory of all equipment assigned to you.

Only use equipment for which you have been granted authorization.

Do not leave computer equipment in a car or in an unsecured location where it might be stolen.

Follow established procedures when removing equipment from NPS premises. This usually includes getting a property pass.

Do not install or use unauthorized software or hardware on NPS information systems, including personal laptop computers, pocket computers or personal digital assistants (PDAs), and network enabled cellular phones.

Do not alter the configuration, including installing software or peripherals, on government equipment unless authorized.

Notify management before relocating computing resources.

Use physical locking devices for laptop computers and use special care for other portable devices.

2.9 Software

Use only software authorized by NPS. Do not install non- NPS standard, public domain or shareware software on NPS computers without approval from the appropriate management official.

Computer users must protect NPS- owned software and protect themselves from malicious software.

Do not use NPS- purchased software on personally owned or non- NPS computers unless

authorized.

Do not alter the configuration, including installing software or peripherals, on government computer equipment unless authorized.

Scan all PC software for viruses using approved, current virus scanning software on a regular basis.

Maintain an inventory of software licenses and media. Keep media in a secure location to prevent theft or unauthorized copying.

Comply with all software licensing agreements and Federal copyright laws.

Unless otherwise expressly authorized, do not download, install, or run security programs or utilities that might reveal weaknesses in the security measures or access privileges of any system.

Employees may use personal software on home computers; however, those computers may not be connected to the NPS network nor may they store any sensitive data.

2.10 Awareness

Annual IT Security Awareness training is mandatory for all NPS employees. New users are required to take the awareness training within two weeks of their start- date.

Employees must stay abreast of security policies, requirements, and issues.

Users must make a conscientious effort to avert security breaches by staying alert to vulnerabilities of NPS information and systems.

Unauthorized computer products in the office (e.g., games, sports pools, personal business software) are prohibited.

Know that you have a right to challenge unauthorized personnel in the work area.

Participate in security training as required.

Read security information available through E- mail, newsletters, memos, and other sources.

Follow all security procedures and comply with all policies related to information security.

If you have questions about the appropriateness of an action or activity, first discuss it with your supervisor or security official.

2.11 Incident Reporting

Report security incidents, or any incidents of suspected fraud, waste or misuse of NPS systems to appropriate officials.

It is each user's responsibility to report any form of security violation, whether it is waste, fraud, or abuse through the NPS incident reporting capability.

Report security vulnerabilities and violations as quickly as possible to proper authorities so that corrective action can be taken.

Take reasonable action immediately upon discovering a violation to prevent additional damage, such as logging out a terminal or locking up property.

Cooperate willingly with official action plans for dealing with security violations.

3. Rules of Behavior - Special Circumstances

The rules below apply to users in special circumstances, consistent with Departmental Guidelines. Your office or manager may add special circumstances at the end of this section.

3.1 Privileged Users

Privileged users are those with one or more of the following functions:

- System administrators
- Computer operators
- System engineers (those with control of the operating system)
- Network administrators
- Data base administrators, and
- Those who control user passwords and access levels.

Privileged users must make an effort to notice the threats to and vulnerabilities of information systems, calling these to the attention of management and working to develop effective countermeasures.

Privileged users will:

- Respond to security alerts and requests by NPS IT security managers
- Protect the supervisor or root- level password at the highest level demanded by the sensitivity of the system
- Use special access privileges only when they are needed to carry out a specific system function
- Whenever possible, use a non- privileged account
- Never use special privileges for personal business, gain, or entertainment
- Use precautionary procedures to protect a privileged account from fraudulent use
- Establish security measures to ensure integrity, confidentiality, and availability of information on systems
- Watch for signs of hacker activity or other attempts at unauthorized access
- Assist with recovery activities and take appropriate action to reduce damage from security violations
- Alert the appropriate personnel when a system goes down or experiences problems
- Ensure that systems and data are properly backed up and that the configuration is adequately documented for recovery purposes.

3.2 Work- at- Home and other Remote Users

Users who are authorized to work in remote locations must take the initiative to understand the security issues related to their work environments. This means staying informed of NPS policies concerning work- at- home. It entails understanding the basics of security across dial- up lines and use of external systems, such as the Internet.

Remote users shall:

- Ensure that adequate security provisions are implemented in your remote work environment
- Establish security at an appropriate level for the equipment and information in your possession. Ensure that confidential data is secure, and that the dial- in access is secure
- Use virus protection software on off- site systems and keep it up- to- date. As appropriate, the NPS will pay the cost of virus protection software
- Be on the alert for anomalies and vulnerabilities, reporting them to proper officials and seeking advice when necessary
- Refrain from altering the configuration, installing software or peripherals, on NPS equipment unless authorized
- Avoid uploading and downloading sensitive information except when required for work
- Use a physical locking device on your laptop computer when appropriate.

3.3 Users who maintain Public Access Sites

Public access sites, especially those based on HTTP and FTP, provide a wealth of information and resources that NPS users can use to great advantage in conducting business. NPS encourages their use for legitimate purposes.

Publicly available information portrays an image of the NPS to the public. Much of the information placed on NPS public access systems represents NPS policy and positions. Information must reflect high rules of integrity. Users must be careful to avoid the appearance of favoritism to or endorsement of any commercial activity.

Security measures must be established to protect the privacy, integrity, and availability of the system and information.

Users who maintain Public Access Sites should observe the following guidelines:

- Use public access systems for official purposes only
- Place only mission- oriented information on a public access system. Do not place personal or unofficial information on a World- Wide- Web (www) page on the Internet, send it via email, or post it on a newsgroup
- Do not allow confidential or sensitive information to be sent, received, or access through public access systems
- Do not place segments of information on public access systems that could be pieced together to infer confidential or sensitive information
- Gain approval through established procedures before placing information on a public

access system

- Ensure that information is accurate and kept up to date
- Do not establish hypertext links between NPS web pages and commercial web pages
- Do not distribute or receive information in violation of copyright laws and intellectual property rights
- Establish a form of access control, such as a firewall, for all servers connected to publicly available networks.

No user, software developer, or Web developer should write or put into production any computer code, program, or script that is considered to be a “Trojan Horse” (applications that attempt to circumvent any security measures) or any other malicious software that would cause harm to the system including viruses, worms, or any “back door” means of accessing the system or applications.

3.4 Contractors and Non-NPS Employee ('Guest User')

Contractors and non- NPS employees may access NPS IT resources, but the rules of behavior are more restrictive than those of an NPS employee, especially in the area of limited personal use of government equipment.

I understand that I am responsible for supporting the network security of the National Park Service (NPS) Network.

I will select network access passwords that are not recognizable, and must contain a combination of numeric, alphabetic and special characters. These passwords will be properly secured at all times. I understand that my network account is for my use only. Neither government employees nor others of my company or agency can use this account.

I understand that creation of 'backdoor' access or dated code will not be permitted.

I recognize that I may have access to data that is within the scope of work and this information may be sensitive. I understand that I have the responsibility to secure this data by distributing the information only when it is required by this scope of work and that it is appropriately identified as NPS 'Confidential' information.

I understand that the NPS has standards and licensing for Information Technology and Systems. I will abide by these licensing practices and will not violate any standards or licensing set forth by law and government standards.

I understand that any data, program coding and scripting, and reports generated by this scope of work will be placed on a designated network drive to insure the information is backed up.

I understand that through the access to the NPS network, I will have access to the Internet. The use of the Internet will be strictly limited to the requirements of the scope of work. I understand that any audio and video streaming technology is not permitted. I understand that network support and security personnel may monitor sessions.

I understand that it is my responsibility (and that of my company or agency) to notify the NPS network administrators of my leaving an assignment.

I understand that failure to follow the above can result in peremptory removal of all network access and may hinder my company's or agency's ability to complete the scope of work.

I understand that I must sign an NPS non- disclosure agreement stating that I will not divulge

personal data or confidential or sensitive information used in performance of my work.

I understand that:

- NPS equipment and networks will be used only to conduct official government business
- Non- NPS equipment (laptop or desktop) will NOT be connected to NPS equipment or networks
- Non- NPS portable media (disks, CD ROMs, etc.) to be used have been checked for and are free of computer viruses and worms
- Non- NPS portable media to be used have been checked for and are free of Individual Indian Trust Data
- The use of NPS IT resources does not involve Individual Indian Trust Data
- The non- NPS user will not permit distribution of any data or information to a non-Federal individual or agency.

4. User Notes

Fill in and retain as a reference for contacting the appropriate staff. Consider including VPN accounts, web e- mail user ID, financial software user IDs, and personnel system user IDs.

System	User ID	Security Contact
Network		
Lotus:Notes		